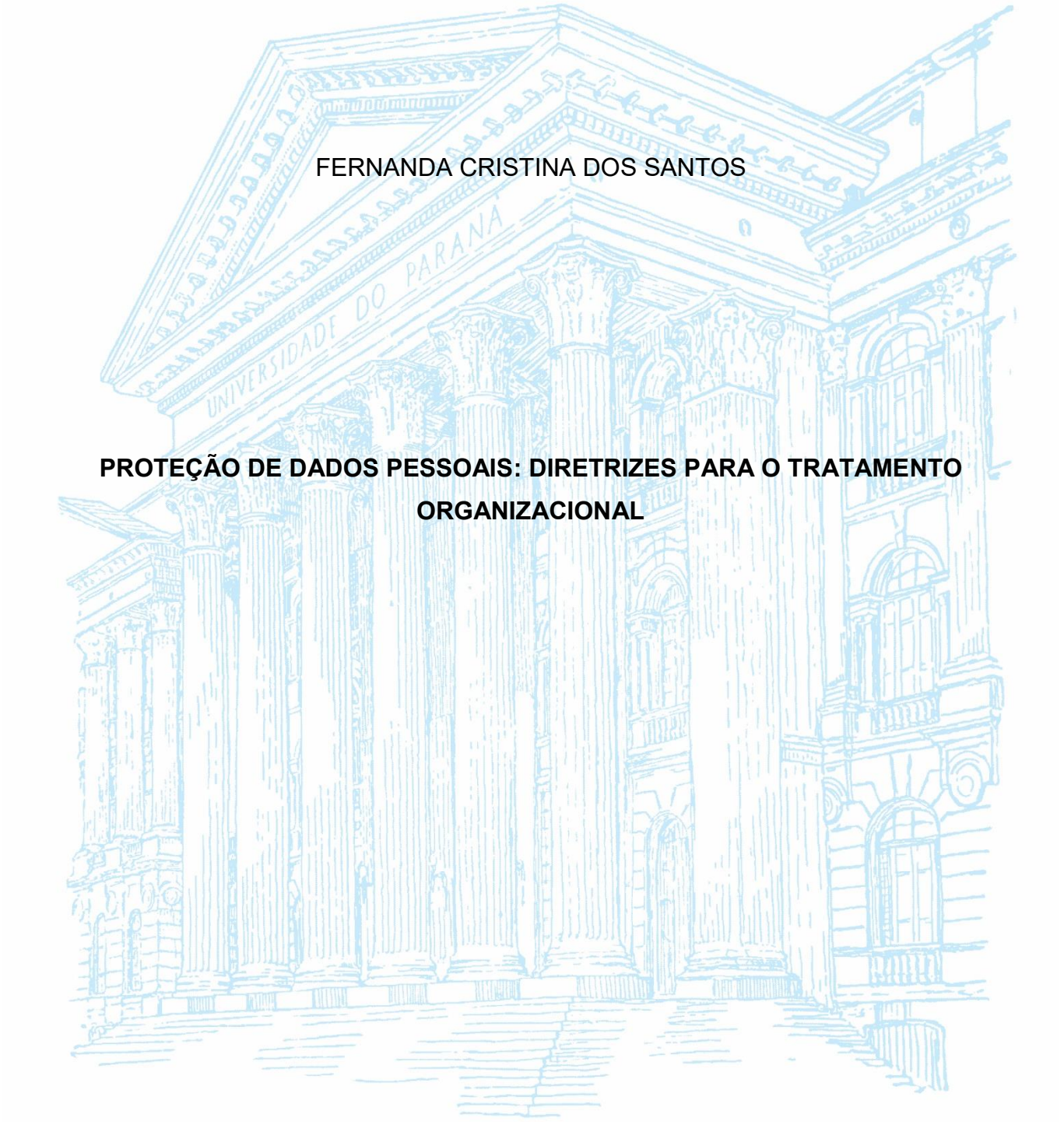
UNIVERSIDADE FEDERAL DO PARANÁ




FERNANDA CRISTINA DOS SANTOS

# PROTEÇÃO DE DADOS PESSOAIS: DIRETRIZES PARA O TRATAMENTO ORGANIZACIONAL

CURITIBA
2017

FERNANDA CRISTINA DOS SANTOS

# PROTEÇÃO DE DADOS PESSOAIS: DIRETRIZES PARA O TRATAMENTO ORGANIZACIONAL

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharela, no Curso de Graduação em Gestão da Informação, Setor de Ciências Sociais Aplicadas, da Universidade Federal do Paraná.

Orientador: Prof. Me. André José Ribeiro Guimarães

CURITIBA

2017

Aos meus pais e irmã, em especial à minha mãe Rosa que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida. A Rafael, obrigada pelo carinho, a paciência e por sua capacidade de me trazer paz em meio à correria dos dias.

## AGRADECIMENTOS

Agradeço a todos os professores que foram essenciais à minha formação como profissional e minha evolução como pessoa. Em especial, ao professor Newton Corrêa de Castilho Júnior, que me orientou no início dessa pesquisa, por todas as contribuições dadas a mim.

Ao meu orientador final, professor André José Ribeiro Guimarães que aceitou este desafio, que me orientou com dedicação e paciência durante todo o processo.

Aos professores Edelvino Razzolini Filho e Mauro José Belli por aceitarem fazer parte desta pesquisa, pela análise crítica e todas as palavras construtivas.

Aos meus colegas de trabalho por me apoiarem e auxiliarem no processo de construção da pesquisa, que será utilizada em nosso meio de trabalho. Espero contribuir da mesma forma.

*“Educação gera conhecimento, conhecimento gera sabedoria, e só um povo sábio pode mudar seu destino.”*

Samuel Lima

## RESUMO

A informação é um bem cada vez mais valorizado, que tem um impacto direto na continuidade e credibilidade do negócio. Neste sentido, esse trabalho apresenta a segurança das informações como estratégia de processos de gestão da informação que oferecem às organizações um maior controle sobre os bens de informações relevantes e conformidade com os mecanismos de confidencialidade. Ressalta que, ao contrário de outros países, inclusive países da América Latina, o Brasil ainda não dispõe de uma lei para regular a coleta, armazenamento, processamento e divulgação de dados pessoais, que no caso desta pesquisa, são as informações sobre seus colaboradores, clientes e fornecedores. Tem o objetivo de identificar quais fatores devem ser contemplados na adoção de práticas específicas para tratamento de dados pessoais de colaboradores, clientes e fornecedores da empresa, utilizando conceitos de segurança da informação no enfoque de gestão da informação. A pesquisa caracteriza-se como estudo descritivo, com abordagem qualitativa, do tipo bibliográfico. Foram realizadas análises detalhadas das leis referentes à América Latina e comparadas entre si para que a pesquisa tivesse uma base sólida com relação às regulamentações. E por fim, apresenta uma proposta de diretrizes para o tratamento das informações ditas pessoais que são utilizadas e processadas pela organização estudada, a partir de diretrizes de tratamento de dados pessoais.



Palavras-Chave: Gestão da Informação. Gestão Organizacional. Tratamento de Dados. Dados Pessoais.

## ABSTRACT

Information is an asset that is increasingly valued, which has a direct impact on the continuity and credibility of the business. In this sense, this work presents information security as a strategy of information management processes that gives organizations greater control over the assets of relevant information and compliance with the confidentiality mechanisms. It emphasizes that, unlike other countries, including Latin American countries, Brazil does not yet have a law to regulate the collection, storage, processing, and dissemination of personal data, which in the case of this research are information about its employees, customers, and suppliers. It aims to identify which factors should be considered in the adoption of specific practices for the treatment of personal data of employees, customers, and suppliers of the company, using information security concepts in the information management approach. The research characterized as a descriptive study, with a qualitative approach, of the bibliographic type. Detailed analyzes of the laws relating to Latin America were carried out and compared so that the research had a solid basis for regulations. Finally, it presents a proposal of guidelines for the treatment of personal information that is used and processed by the organization studied, from personal data treatment guidelines.


Keywords: Information Management. Business Management. Data Processing. Personal Data.

## LISTA DE ABREVIATURAS E/OU SIGLAS

| | | |
|---|---|---|
| ABNT | – | Associação Brasileira de Normas Técnicas |
| CADE | – | Conselho Administrativo de Defesa Econômica |
| COAF | – | Conselho de Controle de Atividades Financeiras |
| CVM | – | Comissão de Valores Mobiliários |
| DPO | – | *Data Protection Officer* |
| GI | – | Gestão da Informação |
| GDPR | – | *General Data Protection Regulation* |
| ISO | – | *International Organization for Standardization* |
| PII | – | *Personally Identifiable Information* |
| PSI | – | Políticas de Segurança da Informação |
| Senacon | – | Secretaria Nacional do Consumidor |
| SI | – | Segurança da Informação |

**SUMÁRIO**

# 1 INTRODUÇÃO

As informações são fundamentais para a sobrevivência organizacional. Por este motivo, é fundamental que sejam tratadas como um dos principais patrimônios existentes na organização. Neste contexto, a Gestão da Informação (GI) é utilizada para gerir os recursos informacionais, e tem a Segurança da Informação (SI) como principal ferramenta para manter o controle sobre os dados relevantes e conformidade com os mecanismos de confidencialidade.

Dentro deste universo, segundo Marciano e Lima-Marques (2006) as organizações estão sujeitas a várias formas de ameaças, que comprometem a segurança das informações, bem como as transações que envolvem o complexo usuário-sistema-informação. As políticas de segurança da informação (PSI) são utilizadas para a preservação no ambiente organizacional, já que abrange variadas áreas de forma adequada, abrangindo recursos computacionais e de infraestrutura e logística, além dos recursos humanos.

As informações ditas externas à organização, como informações pessoais a respeito de colaboradores ou de clientes e fornecedores, tais como nome, data de nascimento e outras descrições da pessoa, ou um número, símbolo, código, imagem atribuídos à pessoa para identificá-la, devem ser tratadas de forma específica. Onde também, se incluem informações que, sozinhas, não conseguem identificar a pessoa, mas conseguem ser verificadas com a mesma facilidade com auxílio de algumas outras informações.

## 1.1 PROBLEMA DE PESQUISA

A proteção da privacidade e dos dados pessoais cada vez mais ganha importância nos dias atuais, o viver em sociedade e a tutela do direito constantemente é desafiada por essas novas questões que se demonstram atuais e efetivas na sociedade da informação. Uma vez que o tema já é realidade em países da América Latina, a tendência é que as empresas brasileiras se preocupem mais com este assunto. As leis existentes no Brasil falham na tarefa de proteger os dados pessoais, segundo Costa (2015) é preciso garantir a disciplina dessa temática de forma democrática, em conjunto com o usuário que dará as diretivas para o tratamento de seus dados pessoais. É necessário disciplinar questão que

atualmente são omissas nas normas existentes, modificar procedimentos para que se cumpra a legislação e não falhem na proteção real de dados pessoais.

A partir do contexto acima, a questão de pesquisa se baseia em: quais fatores devem ser contemplados na adoção de práticas específicas para tratamento de dados pessoais de colaboradores, clientes e fornecedores?

## 1.2 OBJETIVOS

Diante da pergunta formulada, o objetivo geral desta pesquisa é propor diretrizes que contemplem práticas específicas para tratamento de dados pessoais de colaboradores, clientes e fornecedores de uma organização que atua na América Latina. Para atingir este objetivo, foram definidos os seguintes objetivos específicos:

a) Apresentar os conceitos fundamentais da Gestão da Informação e Segurança da Informação no ambiente organizacional;
b) Realizar um levantamento dos países da América Latina que possuem uma lei ou projeto de lei específico para o tema de Segurança de Dados Pessoais;
c) Comparar metodologicamente as leis selecionadas;
d) Elaborar uma proposta de diretrizes que contemplem práticas específicas para tratamento de dados pessoais de colaboradores, clientes e fornecedores.

## 1.3 JUSTIFICATIVA

Este trabalho é baseado nas disciplinas do curso de Bacharelado em Gestão da Informação da Universidade Federal do Paraná, mais especificamente relacionadas aos processos de segurança da informação e processos organizacionais derivados do mesmo. Identificar como essas disciplinas podem auxiliar na adoção de práticas de tratamento de dados pessoais, com oportunidades de melhoria nas regras relativas à gestão da informação no contexto organizacional, baseado na legislação pertinente.

Uma vez que toda empresa possui clientes e parceiros, manter seguras as informações de terceiros vai além de simplesmente evitar o extravio destas. A empresa deve ter o compromisso e a ética em resguardar os dados que estão em

seu poder e saber tratá-las adequadamente e com isso, a melhora da reputação já que demonstra uma preocupação com os dados de seus colaboradores, cliente, fornecedores, etc. Além disso há uma preocupação crescente com dados pessoais e possíveis prejuízos em caso de processos e multas. As pessoas devem saber quais seus direitos sobre seus dados pessoais que são tratados pelas organizações.

## 1.4 ESTRUTURA DO TRABALHO

O trabalho está dividido da seguinte forma: a segunda seção apresenta a revisão teórica, como a abordagem sobre a importância da Gestão da Informação e seus enfoques dentro das organizações; ainda apresenta conceitos de Segurança da Informação e Legislação pertinente: como o Brasil trata sobre o assunto e outras abordagens legais nos contextos latino-americano e mundial. Na terceira seção, são apresentados os procedimentos metodológicos adotados na pesquisa, bem como a classificação da mesma, a descrição do ambiente da pesquisa e o protocolo de análise. Na quarta seção, são apresentados e analisados os resultados obtidos e, por fim, na quinta seção, são apresentadas as considerações finais.

# 2 REVISÃO TEÓRICA

Esta seção apresenta alguns conceitos sobre Gestão da Informação (GI) e Segurança da Informação (SI) no ambiente organizacional. Adicionalmente, o contexto atual é explorado por meio do levantamento de casos relativos à legislação pertinente ao tema. Julga-se importante ressaltar que esta revisão não objetiva o esgotamento dos temas analisados, mas oferecer fundamentos para o entendimento e alinhamento do trabalho.

## 2.1 GESTÃO DA INFORMAÇÃO

Segundo Braga (2000), a informação se tornou uma necessidade crescente para qualquer setor da atividade humana e é indispensável mesmo que a sua procura não seja ordenada ou sistemática, mas resultante apenas de decisões casuísticas e/ou intuitivas. A informação é a base da qual dependem os processos decisórios, porém, se uma empresa para suas atividades por falta de informações por outro lado é importante que a informação seja bem utilizada para o benefício da empresa e que seus processos sejam mais eficientes. Assim, quanto mais importante for determinada informação para as necessidades da empresa, e quanto mais rápido for o acesso a ela, tanto mais essa empresa poderá atingir os seus objetivos. Braga (2000) também afirma que a GI faz a ponte entre a gestão estratégica e a aplicação das Tecnologias de Informação nas empresas, procura, em primeiro lugar, perceber qual a informação que interessa à empresa, para em seguida, definir processos, identificar fontes, modelar sistemas. Neste contexto, as novas Tecnologias de Informação são os instrumentos que permitem gerir a informação em novos moldes, agilizando o fluxo das informações e tornando a sua transmissão mais eficiente (gastando menos tempo e menos recursos) e facilitando, por sua vez, a tomada de decisão.

Segundo Reis (1993, *apud* BRAGA, 2000):

> Para que esta gestão de informação seja eficaz, é necessário que se estabeleçam um conjunto de políticas coerentes que possibilitem o fornecimento de informação relevante, com qualidade suficiente, precisa, transmitida para o local certo, no tempo correto, com um custo apropriado e facilidades de acesso por parte dos utilizadores autorizados (REIS, 1993, *apud* BRAGA, 2000, p. 19).

Segundo Vital, Floriani e Varvakis (2010), a GI requer o estabelecimento de processos, etapas ou fluxos sistematizados e estruturados, associado às pessoas responsáveis por sua condução, para que se obtenham os resultados almejados. Os fluxos de informação permitem o estabelecimento das etapas de obtenção, tratamento, armazenamento, distribuição, disseminação e uso da informação no contexto organizacional.

Segundo Ferreira e Perucchi (2011), um dos objetivos da GI é apoiar as políticas organizacionais, amparando os gestores na tomada de decisão propiciando o aprendizado proposto aos interesses da organização, mediante a construção do conhecimento organizacional. Desse modo, é observado que, sem a gestão, o fluxo de informação que circula nas organizações se dá sem orientação, desperdiçando informações relevantes ao desenvolvimento das organizações.

Para que uma organização atinja seus objetivos de forma eficiente, as informações devem estar alinhadas à estratégia da organização. Ela se apresenta de forma estratégica baseada em três níveis, de acordo com Anthony (1965):

- Nível Estratégico: São tomadas decisões estratégicas; são complexas e exigem informação bastante variada e ao nível das relações da organização/meio envolvente, não se exige muita especificidade. Estão incluídas nela a definição dos objetivos e a elaboração de políticas gerais da organização. A informação provém de fontes externas à organização e também dos outros níveis hierárquicos.
- Nível Tático: São tomadas decisões táticas e exigem informações detalhadas, que provém de fontes internas e sendo obtida com alguma frequência.
- Nível Operacional: São tomadas decisões gerais ou as decisões operacionais. Decisões para problemas bem definidos cuja resolução é, muitas vezes, baseada em fatos atuais e através da aplicação de rotinas. São necessárias informações detalhadas e bem definidas, provenientes essencialmente do sistema interno, com vista a ações imediatas.

Segundo Ferreira e Perucchi (2011), a informação que circula nas organizações percorre um processo que dá acesso ao uso nos variados níveis, e para que esse percurso seja percorrido é necessária a criação de estratégias capazes de dinamizar a informação na estrutura. Choo (2003) afirma que, para criar estratégias de administração da informação, é útil elaborar os processos que

compreendem essas amplas categorias. A análise da administração da informação é feita, de acordo com o autor, mediante um ciclo contínuo de seis processos correlatos: 1) Identificação das necessidades de informação; 2) Aquisição da informação; 3) Organização e armazenamento da informação; 4) Desenvolvimento de produtos e serviços de informação; 5) Distribuição da informação e; 6) Uso da informação. Para a prática do ciclo contínuo na criação de estratégia, para Ferreira e Perucchi (2011), as organizações passaram a aderir uma nova postura em relação à informação.

> O acesso e uso imediatos da informação oferecem condições acerca das decisões no que tange à coordenação eficaz em processos de recursos humanos, de comunicação, de aprendizagem, de inovação, de redução de custos apresentados pela dificuldade de coleta, organização, armazenamento, compartilhamento e utilização da informação circular intra e interorganizacional. Esse comportamento, de acordo com as autoras, possibilita às organizações a se posicionarem como organizações competitivas. (FERREIRA e PERUCCHI, 2011, p. 3).

McGee e Prusak (1994) descrevem a competitividade, nos dias atuais, como fator que tem como base a capacidade de recuperar, tratar, interpretar e utilizar a informação de forma eficaz. Portanto, gerenciar informação, pode ser entendido como a definição e criação de ações, mediante um contexto informacional interno e externo às organizações que dela necessitem. Choo (2003) conclui que a administração (gestão) da informação seja vista como a administração de uma rede de processos que adquirem, criam, organizam, distribuem e usam a informação.

### 2.1.1 Políticas de Informação como estratégia de Gestão da Informação

Ainda é raro encontrar organizações que tenham políticas de informação explícitas, ou seja, um documento formal com diretrizes, regras e princípios adotados relacionados aos processos corporativos. As políticas de informação e de segurança de informação orientam a análise de riscos que é, segundo Beal (2008), o processo no qual são avaliadas as ameaças existentes, as probabilidades de acontecer e os impactos para o negócio, a fim de se poder determinar os requisitos de segurança a serem supridos por controles (medidas de proteção).

Um princípio que pode ser considerado em uma política de informação corporativa é o exemplo dado por Davenport e Prusak (2001):

> Uma orientação mercadológica quase sempre implica uma administração descentralizada dos recursos informacionais: os proprietários podem nomear, formatar, atualizar e ordenar as informações como desejarem. Fornecedores de informação e facilitadores podem encarregar-se de quaisquer informações ou serviços pelos quais os clientes estiverem dispostos a pagar, a preços de mercado. (DAVENPORT e PRUSAK, 2001, p. 102).

A existência de uma política de informação formal auxilia a organização de muitas formas, inclusive quanto à ética na utilização dos dados corporativos. Para Dantas (2001), pode-se definir a política de segurança como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações.

Na seção a seguir, será tratado sobre a Política de Segurança da Informação após a contextualização sobre Segurança da Informação.

## 2.2 SEGURANÇA DA INFORMAÇÃO

As informações são bens organizacionais e a segurança da informação é um recurso relevante que traz proteção aos ativos. Cada organização define qual estrutura será adequada e condizente com seu porte e seu tipo de negócio, para a proteção de seus dados e informações. A Segurança da Informação (SI) existe para minimizar riscos em relação à dependência do uso dos recursos de informação para o fluxo correto dos processos organizacionais. Ou seja, sem a informação ou com dados incorretos, acarretará em perdas para o negócio. Por isso é necessário avaliar que tipo de informações terá a necessidade de cuidados com a proteção. Abreu (2001) classifica a informação em níveis de prioridade, respeitando a necessidade de cada empresa assim como a importância da classe de informação para a manutenção das atividades da empresa:

- Pública: Informações que podem ser divulgadas sem consequências danosas ao funcionamento da organização, e cuja integridade não é vital.
- Interna: O acesso deste tipo de informação não deve ser livre, embora uma possível divulgação não traga consequências graves. A integridade é importante mesmo que não seja vital.

- Confidencial: Informação restrita à organização, cuja divulgação ou perda pode levar a consequências operacionais, como perdas financeiras ou de confiabilidade perante clientes, por exemplo.
- Secreta: Informação crítica para a organização e suas atividades, sua integridade deve ser preservada a qualquer custo e seu acesso deve ser restrito às pessoas autorizadas. A segurança deste tipo de informação é vital para a companhia. Conforme Sá (2001), a divulgação das informações confidenciais ou secretas pelos elementos que participam da organização é considerada falta de ética e moral grave.

Albuquerque e Ribeiro (2002) afirmam que há três princípios básicos para garantir a SI:

- Confidencialidade: A informação só pode ser acessada por pessoas autorizadas. Confidencialidade é a proteção contra pessoas não autorizadas a acessarem informações.
- Disponibilidade: A informação deve estar disponível quando for necessária a sua utilização.
- Integridade: A recuperação da informação deve estar em formato original, como no momento em que foi armazenada. Protege os dados ou informações contra modificações intencionais ou acidentais não autorizadas.

Para Laureano e Moraes (2005), alguns autores defendem que para que uma informação seja considerada segura, o sistema que o administra ainda deve respeitar os seguintes critérios:

- Autenticidade: Garante que a informação é autêntica.
- Não repúdio: Não é possível negar uma operação ou serviço que modificou ou criou uma informação.
- Legalidade: Garante a legalidade jurídica da informação, onde todos os ativos estão de acordo com a legislação vigente.
- Privacidade: Não pode ser confundida com confidencialidade, uma informação privada somente pode ser acessada e alterada por seu dono.
- Auditoria: Rastreabilidade dos passos de um processo, identificando os participantes, os locais e horários de cada etapa. A auditoria traz

credibilidade e é responsável pela adequação da empresa às políticas legais e internas.

No passado, a SI era apenas tratada em meios tecnológicos, porém hoje o desafio das organizações é construir uma relação de confiabilidade com clientes e fornecedores. Conforme afirmam Rezende e Abreu (2000), as empresas estão procurando dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório. A adoção de políticas de segurança de informação proporciona transparência e fornece credibilidade à organização perante seus colaboradores e a sociedade.

A prática de SI dentro das organizações deve ser orientada pelas Políticas de Segurança da Informação que abrangem as diversas áreas do contexto organizacional, como recursos computacionais e até recursos humanos. Elas têm o papel de informar um código de conduta às quais os colaboradores devem se adequar totalmente e serão abordadas no próximo tópico. Segundo Marciano e Lima-Marques (2006), a correta gestão ou governança é atingida quando há compromisso de todos com as normas e procedimentos estabelecidos.

### 2.2.1 Política de Segurança da Informação

Como mencionado na seção 2.1.1, as políticas informacionais são de extrema importância para as organizações e para a segurança sobre a manipulação e utilização dos dados e informações. Para Beal (2008), a adoção de uma PSI surge da necessidade de empregar diretrizes e regras para o acesso e manipulação da informação para a proteção dos dados. Ela deve identificar claramente as responsabilidades em relação à SI em todos os níveis organizacionais. Embora o conteúdo varie de acordo com a organização, ela deverá abranger, sempre que cabível, os seguintes aspectos conforme a autora:

- Estrutura de Segurança: Orientações sobre estrutura de gestão para o planejamento e controle da segurança das informações, deixando claro quem são os responsáveis, em todos os níveis da organização.
- Classificação e Controle: Orientações sobre as informações classificadas como críticas e responsabilidades para a manutenção dos controles sobre as mesmas,

- Aspectos Humanos: Definições sobre a política de segurança pessoal (processos de admissão e demissão) e de treinamento em segurança informacional; diretrizes de comportamento esperado em relação aos recursos computacionais disponíveis e em caso de ocorrência de incidentes de segurança.
- Segurança Física e do Ambiente: Diretrizes para a proteção dos recursos e instalações de processamento de informações críticas ou sensíveis para o negócio contra acessos não autorizados, danos ou interferências.
- Gestão das Operações e Comunicações: Diretrizes para garantir a operação correta e segura do processamento das informações, proteger a integridade dos serviços e informações e assegurar a conexão segura com sistemas externos.
- Controle de Acesso: Diretrizes para o monitoramento e controle de acesso aos recursos da rede e de aplicativos, para prevenir abusos internos e ataques externos.
- Prevenção e Tratamento de Incidentes: Diretrizes para prevenção, detecção e investigação de incidentes de segurança, bem como a emissão de relatórios dos mesmos.
- Desenvolvimento, implantação e manutenção de sistemas: Diretrizes para uso de controles de segurança em todas as etapas do ciclo de vida dos sistemas.
- Gestão da Continuidade dos Negócios: Diretrizes para que a organização se prepare para neutralizar interrupções nos processos críticos na ocorrência de falhas ou desastre.
- Conformidade: Diretrizes para a preservação da conformidade com requisitos legais (tais como proteção de direitos autorais e da privacidade), normas e diretrizes internas (incluindo o tratamento de informações proprietárias) e requisitos técnicos de segurança. Indicação das punições a serem adotadas em caso de violação da política de segurança (advertências, demissão por justa causa ou até ação judicial).

Segundo Beal (2008), uma PSI não deve ser estática, para que seja sempre efetiva ela deve acompanhar as mudanças nas necessidades do negócio. É

necessário que além das diretrizes acima, também se estabeleça periodização de atualizações do documento.

### 2.2.2 Proteção de Dados e Informações Pessoais

Além da preocupação com a segurança de informações gerais, as organizações devem proteger com maior atenção os dados pessoais coletados de clientes, funcionários e outros cadastrados em seus bancos de dados. Segundo Rouse (2014), Informações de Identificação Pessoal (*Personally Identifiable Information* – PII) referem-se a informações que podem ser usadas para identificar, contatar ou localizar uma única pessoa. Também podem ser usadas com outras fontes para identificar um único indivíduo. A autora conclui que a organização tem o compromisso de utilizar estes dados para objetivos previamente especificados e autorizados pelo dono da informação, não devendo ser mantidas nas bases de dados da organização, sem que haja necessidade ou que não sejam exigidas legalmente para o funcionamento do negócio. A declaração formal dos propósitos da coleta e do armazenamento de dados de clientes (como a manutenção de cadastros, cobrança, etc.), das formas em que eles podem ser usados ou compartilhados com terceiros, do tipo de dado que deve ser preservado ou descartado, pode reduzir os riscos de uso antiético das informações.

Segundo Rouse (2014), há algumas informações que são difíceis de identificar e devem ser restritas ao ambiente da organização ou, no máximo, podem ser eventualmente divulgadas. É nesse tipo de situação em que golpes ou fraudes podem acontecer ao divulgar este tipo de informação e a organização sempre sairá prejudicada, porque foi vítima da fraude ou porque permitiu que os dados fossem utilizados indevidamente. Podendo evidenciar a falta de proteção dos dados e comprometendo a ética e a imagem da organização, em alguns casos isso também acarretará medidas judiciais. A legislação sobre o assunto será abordada no tópico a seguir.

## 2.3 LEGISLAÇÃO PERTINENTE

O Anteprojeto de Lei de Proteção de Dados Pessoais foi elaborado pela Secretaria Nacional do Consumidor (Senacon), em conjunto com a Secretaria de Assuntos Legislativos do Ministério da Justiça, após a realização de dois debates públicos, realizados via internet. O primeiro em 2010 e o segundo no ano de 2015, após cinco anos de estudos e debates públicos. Além de duas consultas públicas, o governo federal recebeu aproximadamente 1,3 mil contribuições sobre o assunto, de diversos setores da sociedade, para a formulação da proposta. A falta de legislação dá espaço para que muitas empresas utilizem de forma abusiva informações pessoais da população. Segundo o Portal Brasil (2015), naquele ano 109 países já tinham a disposição leis para proteger o cidadão do uso inadequado de informações pessoais, segundo o Ministério da Justiça. Desses países, 90% já contavam com órgãos para fiscalização do uso.

O Marco Civil da Internet (Lei nº 12.965 de 2014) que regula o uso da rede e garante privacidade, atua apenas no ambiente da internet. E a segurança destes dados vai além do computador, está em todo lugar de diferentes maneiras. Com a lei, a coleta de dados apenas acontece sob consentimento, assim como o armazenamento e o tratamento dado às informações pessoais, por qualquer que seja a instituição, desde financeira até redes sociais. Segundo o Portal Brasil (2015), muitas empresas criam bancos com os dados das pessoas, e vendem para outras companhias que têm interesse naquelas informações. Segundo a Agência Senado (2015), o cidadão também deve ter direito de se opor ao tratamento imposto a seus dados; de não ter seus dados fornecidos a terceiros, a não ser em casos de consentimento prévio; de conhecer a finalidade do tratamento automatizado dos seus dados ou mesmo de requerer a exclusão definitiva de suas informações pessoais armazenados após o término dos contratos com empresas.

O texto do anteprojeto de lei diferencia dados pessoais, sensíveis e anônimos. Segundo o Senado (2015), o projeto proíbe a coleta e uso de dados anônimos que possam ser identificados a partir de cruzamento de informações. Também não permite o tratamento de dados que revelem orientação (religiosa, política ou sexual), convicção (filosófica) ou origem racial ou étnica, entre outros, a menos que haja consentimento expresso do titular. A proposta determina ainda que o tratamento de dados pessoais de crianças ou pessoa absolutamente incapaz

somente pode ser realizado mediante consentimento dos responsáveis legais e no seu melhor interesse.

Segundo Faustino (2016) essas garantias já estão previstas na Constituição Federal de forma abrangente e/ou em leis com escopos específicos (como o Código do Consumidor, lei do Cadastro Positivo, etc.). O PL, no entanto, vem estabelecer alguns princípios para nortear o tratamento de dados pessoais. Podemos destacar, a exemplo, o princípio da finalidade específica, adequada e necessária, segundo o qual o tratamento deve ser realizado para fins legítimos e específicos, e limitado ao necessário para este fim; e, os princípios da segurança e livre acesso, pelos quais o responsável pela coleta dos dados deve mantê-los em total proteção, permitindo, no entanto, o acesso ao seu titular, o qual deve dar consentimento livre e inequívoco para que o tratamento dos dados seja considerado legítimo.

Uma vez aprovada, a lei será aplicada mesmo que a atividade seja realizada por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos um integrante do mesmo grupo econômico possua estabelecimento no Brasil. Da mesma forma, se a coleta, o armazenamento ou a utilização dos dados pessoais ocorrer em local onde seja aplicável a lei brasileira por força de tratado ou convenção. Os responsáveis pelo tratamento de dados pessoais respondem, independentemente da existência de culpa, pela reparação dos danos causados aos titulares ou a terceiros. Os proprietários ou gestores de banco de dados devem adotar medidas destinadas à proteção dos dados pessoais contra a perda ou destruição acidental ou ilícita, a alteração, a difusão e o acesso não autorizados. Para isso, precisam impedir que pessoas não autorizadas tenham acesso aos equipamentos, instalações e suportes de tratamento de dados; garantir que somente pessoas autorizadas tenham acesso aos dados transmitidos; e garantir a possibilidade de verificação periódica das alterações produzidas nos arquivos de dados.

Atualmente no Brasil, as regras estão fragmentadas em diversos órgãos, como na Comissão de Valores Mobiliários (CVM), Conselho Administrativo de Defesa Econômica (CADE), Conselho de Controle de Atividades Financeiras (COAF) e Secretaria Nacional do Consumidor (Senacon), que não contemplam todas as atividades. O Brasil perde financeiramente em negócios por não ter regras convergentes de proteção de dados, o que dificulta especialmente o comércio com países europeus e os Estados Unidos, segundo o representante da Open

Knowledge Foundation, Danilo Denoda em entrevista à Lucia Berbert (2017), do Teletime. Ele ainda diz que o Brasil está atrasado sobre a questão da privacidade dos dados até na América Latina, onde países como o Uruguai e a Argentina saíram na frente.

Existem diversas leis em outros países que protegem o dono da informação e obrigam as empresas que possuem os dados a realizar controles de segurança, e no caso de não cumprimento da mesma, multas expressivas são aplicadas se alguém for lesado. Dentre as leis existentes, uma das mais abrangentes sobre o assunto é a LOPD - *Ley Orgánica de Protección de Datos de Carácter Personal* da Espanha, que foi decretada pelo Rei Juan Carlos, em 2007, complementando a lei de 1999. Segundo Galvão (2010), ela trata de assuntos como a Qualidade de Dados, incluindo a integridade dos mesmos; o Direito do Acesso à Informação, incluindo controle de quem poderá acessar e tempo de disponibilização; Termo de Autorização, incluindo o informe sobre o tipo de tratamento que seu dado terá; o Acesso por Terceiros, incluindo autorizações e aprovações necessárias à concessão de acesso; a Exclusão de Informações, onde os dados devem ser excluídos após um determinado tempo; o Monitoramento através de câmeras de vídeo ou qualquer outro tipo em que seja possível identificar uma pessoa; a Transferência Internacional de Dados, onde são tratadas todas as regras, aprovações e controles necessários para o intercâmbio, envio ou armazenamento de dados em outro país que não possua legislação específica sobre o assunto. A multa por descumprimento pode chegar a 600 mil euros, de acordo com o tipo de informação e consequências geradas.

Em 2016 a União Europeia aprovou a GDPR (*General Data Protection Regulation* – Regulamentação Geral de Proteção de Dados), conforme notícia publicada no site Advisera em outubro de 2016 por Carla Bouca, que substituirá a atual Diretiva (Diretiva de Proteção de Dados 95/46/EC) que não era atualizada desde 1995. Esta nova regulamentação (EU GDPR) foi aprovada em 14 de abril de 2016, pelo Parlamento Europeu e Conselho da Europa e será aplicada diretamente em cada país, permitindo uma consistência de regras entre nações sobre os direitos de privacidade dos cidadãos. Alguns dos mais relevantes pontos são os seguintes: Levar em conta a natureza e o propósito do uso dos dados, tanto aqueles que determinam o propósito e meios de processamento de dados pessoais (Controladores de Dados), como aqueles que por sua vez podem gerenciá-los

(Processadores de Dados), para estar em conformidade com a EU GDPR, terão que implementar medidas organizacionais e técnicas para atingir um nível apropriado de segurança de dados em termos de confidencialidade, integridade, disponibilidade e resiliência dos sistemas que os suportam, assim como a validação regular da eficácia destas medidas. Pela nova regulamentação, as organizações têm que minimizar a coleta e retenção de dados e obter consentimento dos consumidores quando do processamento dos dados – em outras palavras, minimizar a coleta de dados do consumidor, minimizar com quem os dados são compartilhados, e minimizar por quanto tempo é mantido. A meta é que as organizações coletem ou armazenem apenas informações que elas precisam para o propósito pretendido, particularmente com relação a dados pessoais; Se a organização lida com categorias especiais de dados pessoais em larga escala, ela precisa designer um DPO (Data Protection Officer – Gestor de Proteção de Dados) como parte de sua diretoria; Se estas medidas não forem atendidas, as penalidades são altas: até 20 milhões de Euros ou em caso de organizações, até 4% do volume anual de negócios, o que for mais alto.

A ISO/IEC 27001 é a norma internacional de gestão de segurança da informação. Conforme a BSI - British Standards Institution, ela descreve como colocar em prática um sistema de gestão de segurança da informação avaliado e certificado de forma independente. Isso permite que você proteja todos os dados financeiros e confidenciais de maneira mais eficiente, minimizando a probabilidade de serem acessados ilegalmente ou sem permissão. Embora fundamental para a Segurança da Informação, a família ISO 27000 não trata diretamente sobre dados pessoais, são citados conceitos relacionados como confidencialidade e estar de acordo com as leis e regulamentações relevantes, de acordo com a listagem a seguir:

- ISO/IEC 27001:2005 – foi publicada em 2005 e aborda sobre Tecnologia da Informação, Técnica de Segurança e Sistemas de gestão de segurança da informação.
- ISO/IEC 27002:2005 – foi publicada em 2005 e tem como título diferenciado o Código de prática para a gestão de segurança da informação. Ela estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação. Os objetivos definidos nela provêm diretrizes gerais sobre as metas geralmente aceitas para SGSI.

- ISO/IEC 27003:2010 – foi publicada em 2011 e aborda os seguintes tópicos: Tecnologia da Informação, Técnicas de segurança e Diretrizes para implantação de um Sistema de Gestão de Segurança da Informação (SGSI).
- ISO/IEC 27004:2009 – foi publicada em 2010 e acrescenta os títulos Gestão da segurança da informação e a Medição.
- ISO/IEC 27005:2008 – foi publicada em 2008 e acrescenta nos seus títulos a questão da Gestão de riscos de segurança da informação.
- ISO/IEC 27011:2008 – foi publicada em 2009 e tem como objetivo fornecer diretrizes para a gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002.

Embora consultadas, as normas da ABNT são normas técnicas, enquanto as leis, que são objeto de estudo nesta pesquisa, são normas jurídicas ou legais. As diferenças entre as duas passam pelos seus objetivos e campos de competências principalmente. A ABNT é a entidade reconhecida como competente, em nosso país, para enunciar as normas técnicas, e as suas normas constituem-se referência e exigência em algumas normas jurídicas, como a Lei n° 8.078, de Proteção e Defesa do Consumidor. Porém não tem caráter jurídico e/ou obrigatório.

# 3 METODOLOGIA

A seguir, são apresentados os procedimentos metodológicos para a realização da pesquisa. Sua classificação, ambiente da pesquisa e por fim a coleta e o tratamento dos dados.

## 3.1 CLASSIFICAÇÃO DA PESQUISA

Para este estudo, pode-se classificar a pesquisa, segundo a natureza, como uma pesquisa aplicada, com o objetivo de gerar conhecimento para aplicação prática, dirigida à solução do problema apresentado.

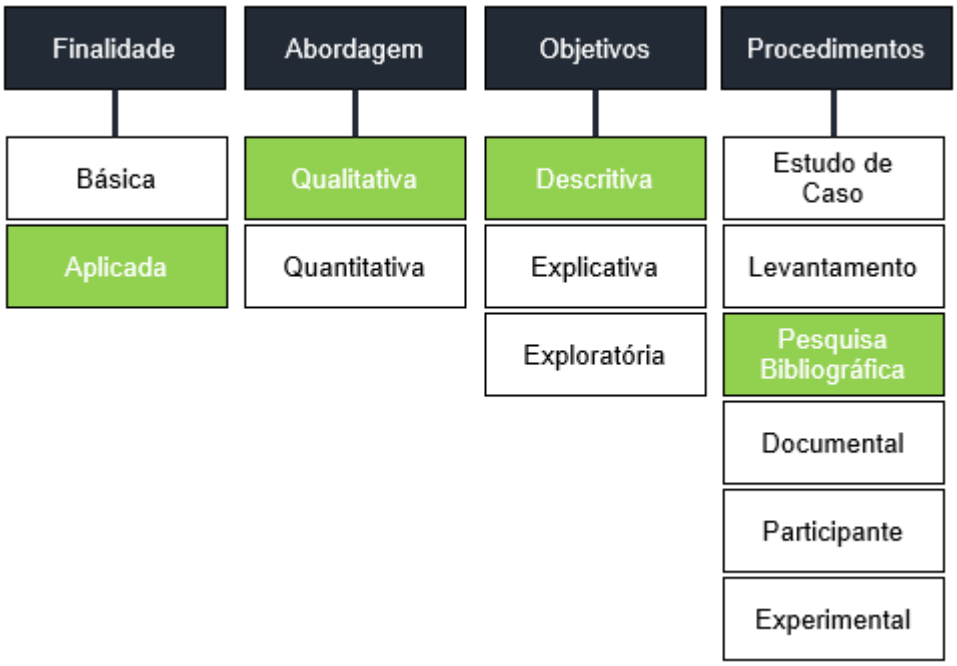
Quanto à abordagem, foi utilizada a pesquisa qualitativa, que segundo Silva e Menezes (2005) considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. Não foram utilizados métodos e técnicas estatísticas, a análise dos dados foi realizada indutivamente pela pesquisadora, já que a fonte da coleta de dados foi o ambiente natural.

Em relação aos objetivos, a presente pesquisa é classificada como descritiva, pois, segundo Silva e Menezes (2005), visa descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. A autora complementa que este tipo de pesquisa busca descrever um fenômeno ou situação em detalhe e abrange com exatidão as características de um indivíduo, uma situação, ou um grupo, bem como desvenda a relação entre os eventos.

Enquanto procedimento, este trabalho realizou-se por meio de uma pesquisa bibliográfica que se utiliza de materiais já publicados, constituído de livros, artigos de periódicos e atualmente com material disponibilizado na Internet. E também por uma pesquisa participante, porque o pesquisador tem acesso às informações dentro da organização. Segundo Campos (2004) a análise de conteúdo como conjunto de técnicas se vale da comunicação como ponto de partida. Diferente de outras técnicas como a estocagem ou indexação de informações, a crítica literária, é sempre feita a partir da mensagem e tem por finalidade a produção de inferências.

A Figura 1 mostra a classificação final da pesquisa de acordo com as classificações abordadas por Silva e Menezes (2005).

FIGURA 1 - CLASSIFICAÇÃO DA PESQUISA




FONTE: A Autora (2017).

## 3.2 AMBIENTE DE PESQUISA

A organização X é uma empresa multinacional japonesa, do setor industrial de telecomunicações e tecnologia há mais de 40 anos no mercado brasileiro. Localizada na Cidade Industrial de Curitiba, hoje possui mais de 1000 funcionários somente nesta planta. A demanda desta pesquisa surgiu da necessidade de atender requisitos de Segurança de Informação Pessoal para a filial Colombiana, já que todas as informações pessoais de colaboradores, fornecedores e clientes colombianos são repassadas às equipes responsáveis na matriz brasileira e são armazenadas em Banco de Dados. A transferência internacional de dados deverá ser tratada com regras, aprovações e controles para o intercâmbio, envio ou armazenamento de dados onde não haja legislação específica sobre o assunto, como é o caso do Brasil.

## 3.3 COLETA E TRATAMENTO DE DADOS

O resultado esperado deste trabalho é a apresentação de uma proposta de melhoria dos processos de Segurança da Informação para o tratamento de dados pessoais de colaboradores e/ou clientes e fornecedores. Como instrumento de coleta de dados utilizou-se registros institucionais, com o levantamento e análise de políticas e procedimentos já existentes sobre Segurança da Informação; mapeamento de quais pontos da lei que não estão cobertos pelos processos existentes e propor mudanças de processo e documentos como novos procedimentos e política específica de segurança de dados pessoais. Uma das primeiras fontes de informação consideradas foi a existência de registros na própria organização, sob a forma de documentos, fichas, relatórios ou arquivos em computador. O uso de registros e documentos já disponíveis reduz tempo e custo de pesquisas para avaliação. Além disto, esta informação é estável e não depende de uma forma específica para ser coletada. Foram realizadas análises detalhadas das Leis referentes à América Latina e coletados seus itens mais importantes para que a proposta tivesse uma base sólida com relação as regulamentações.

# 4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

A seguir é apresentada a análise dos resultados obtidos a partir da pesquisa.

## 4.1 ANÁLISE DOS PROJETOS DE LEIS

A proposta de Política de Segurança de Dados Pessoais foi baseada nos princípios das leis existentes nos países da América Latina, principal área atuação da empresa X, e na proposta de lei Brasileira, considerando a matriz brasileira da organização. Para isso, foram analisadas as seguintes leis:

- Ley nº 25.326 – Protección de los Datos Personales (Argentina, 2000): Dispões sobre os princípios gerais relativos a proteção de dados, responsabilidade sobre o arquivamento, registro e banco de dados, controle e ações de proteção sobre os dados pessoais.
- Decreto Supremo nº 1.793 - Reglamento para el Desarrollo de tecnologías de Información y Comunicación (Bolívia, 2013): A Bolívia trata este assunto como um tópico do regulamento em complemento à Lei nº 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicaciónes, apenas cobre informações que estão em meios tecnológicos, têm como padrão de tratamento de dados pessoais: qualquer operação ou conjunto de operações sobre dados pessoais como a coleta, armazenamento, uso, divulgação ou supressão.
- PL 5.276/2016 - Anteprojeto de Lei de Proteção de Dados Pessoais (Brasil, 2016): Este projeto de lei dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- Ley nº 19.628 - Protección de Datos de Carácter Personal (Chile, 1999): O processamento de dados pessoais em registros ou bancos de dados por órgãos públicos ou indivíduos deve estar sujeito às disposições da lei. Qualquer pessoa pode processar dados pessoais, desde que o faça de forma consistente com esta lei e para fins permitidos. De qualquer modo, deve respeitar o pleno exercício dos direitos fundamentais dos proprietários de dados e os poderes que esta lei os reconhece.

- Ley nº 1.581 - Protección de Datos Personales (Colômbia, 2012): Lei sobre o direito constitucional que todas as pessoas têm de conhecer, atualizar e retificar suas informações que estão em banco de dados ou arquivos, e os demais direitos, liberdade e garantias. Os princípios de proteção de dados devem ser aplicados a todos os dados, incluindo os armazenados em bancos de dados.
- Ley Federal de Protección de Datos Personales Posesión de los Particulares (México, 2010): Esta lei é de ordem pública e de observância geral em toda a República e proteção de dados pessoais detidos por particulares, com o objetivo de tratamento legítimo, controlado e informado, a fim de garantir a privacidade e o direito à autodeterminação das pessoas.
- Ley nº 18.331 – Protección de Datos Personales y Acción de “Habeas Data” (Uruguai, 2008): A lei é aplicável aos dados pessoais registrados em qualquer meio que os torne suscetíveis ao tratamento e a qualquer modalidade de uso subsequente desses dados por áreas públicas ou privadas.

A Tabela 1 apresenta o comparativo entre as leis que foi elaborado a partir doa identificação dos principais tópicos abordados:

QUADRO 1 – COMPARATIVO AMÉRICA LATINA

| Tópicos | Argentina | Bolívia | Brasil | Chile | Colômbia | México | Uruguai |
|---|---|---|---|---|---|---|---|
| Autorização do Titular | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Finalidade, Disponibilização e Destino | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Princípios de Segurança de Dados | - | ✓ | ✓ | - | ✓ | ✓ | ✓ |
| Armazenamento de Dados | ✓ | × | - | ✓ | ✓ | ✓ | ✓ |
| Modificação de Dados | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| Anonimização de Dados | × | × | ✓ | × | × | × | × |
| Bloqueio/Eliminação de Dados | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| Transferência de Dados | ✓ | × | ✓ | × | ✓ | ✓ | ✓ |
| Fiscalização | ✓ | × | - | × | ✓ | × | - |

Fonte: A Autora (2017).

Cada lei aborda os tópicos levantados de forma específica. Na proposta realizada, foi considerada a maior abrangência de itens e detalhes sobre todas as leis (e projeto de lei) estudados. Todas as leis dispõem sobre a autorização expressa do titular para o responsável pelo tratamento da informação, bem como deve ser informado ao titular que a informação será tratada, com finalidade de registro, informando que será disponibilizada e a quem será disponibilizada. Sobre os princípios de Segurança de Dados, apenas a lei chilena não engloba conceitos base sobre os princípios, apesar de abordar os deveres de outra forma. Para o

tratamento dos dados pessoais (armazenamento, modificação, bloqueio, eliminação) as leis possuem disposições e obrigações dos responsáveis sobre os dados. Tendo a obrigação de prestação de informações para o titular, em qualquer uma destas situações. A anonimização de dados apenas aparece no projeto de lei brasileiro, trata sobre a anonimização a partir dos dados obtidos (informações que não identificam o titular). A transferência de dados, ponto principal da política proposta, é abordada nas leis colombiana e mexicana, bem como no projeto de lei brasileiro. A fiscalização, com penalidades específicas, apenas é abordada na Colômbia. A seguir, foi abordado cada termo em específico para o entendimento da importância e como cada lei ou projeto de lei se refere ao mesmo.

### 4.1.1 Autorização do Titular

Define-se como autorização o ato ou efeito de autorizar; consentimento, permissão (MICHAELIS, 2017). Ordem ou determinação pela qual se autoriza ou se concede poder ou licença. Todas as leis são unânimes ao tratar sobre a autorização do titular, a lei argentina regula que o responsável pelo tratamento deve ter o consentimento prévio, expresso e informado do titular para realizar o processamento de dados pessoais, que deverá constar por escrito ou por outro meio que se equipare, de acordo com as circunstâncias.

A lei boliviana regula que todas as pessoas a quem as informações pessoais são solicitadas devem ser previamente informadas que seus dados serão processados, o objetivo da necessidade, registro e possível transmissão. Informar ao titular a identidade e o endereço do responsável pelo tratamento e os direitos de acesso, retificação, atualização, cancelamento, objeção, revogação e outros que sejam pertinentes. Os dados pessoais sujeitos a tratamento não podem ser utilizados para fins diferentes daqueles expressados no momento da coleta e registro.

O projeto de lei brasileiro define como autorização a “manifestação livre e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. Para os dados sensíveis apenas serão tratados aqueles que forem fornecidos pelo titular com consentimento inequívoco, expresso e específico pelo titular e/ou com informação prévia e específica sobre a natureza

sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no seu tratamento.

A lei chilena regula que a autorização deve ser por escrito e o titular deve estar devidamente informado sobre o propósito do armazenamento de seus dados pessoais e sua possível transmissão. Ela pode ser revogada, sem efeito retroativo, também sendo feito por escrito pelo titular. Não é requerido autorização para as informações pessoais provenientes ou coletadas de fontes acessíveis ao público.

A lei colombiana regula que o responsável pelo tratamento deve ter o consentimento prévio, expresso e informado do titular para realizar o processamento de dados pessoais.

A lei mexicana regula que todo o processamento de dados pessoais estará sujeito ao consentimento de seu proprietário. O consentimento é entendido quando a vontade for expressa verbalmente, por escrito, por meio eletrônico, óptico ou qualquer outra tecnologia e o mesmo poderá ser revogado a qualquer momento sem efeitos atribuídos. No caso de dados pessoais sensíveis, que a lei trata como os dados cujo uso indevido pode dar origem a discriminação ou implicar um risco grave para seu titular. O responsável deve obter o consentimento expresso e por escrito do titular para o seu tratamento, através de assinatura eletrônica, ou qualquer mecanismo de autenticação estabelecido para este fim.

A lei uruguaia regula que o processamento de dados pessoais é lícito quando o proprietário deu seu consentimento livre, prévio, expresso e informado, que deve ser documentado.

### 4.1.2 Finalidade, Disponibilização e Destino

Como parte dos princípios de Segurança de Informação, a finalidade, a disponibilidade e o destino dos dados pessoais devem ser informados e consentidos pelo titular. A lei argentina regula que os titulares devem ser previamente informados de forma expressa e clara sobre a finalidade, a existência do arquivamento e a possibilidade que o titular tem de acessar, retificação e supressão de seus dados.

A lei boliviana regula que os titulares devem ser previamente informados sobre os objetivos do registro, dos possíveis destinatários da informação e que os mesmos não podem ser utilizados para fins diferentes daqueles expressados no momento da coleta.

O projeto de lei brasileiro trata que o titular deverá ter acesso às informações sobre o tratamento de seus dados, como: finalidade específica do tratamento; forma e duração do tratamento; identificação do responsável; informações de contato do responsável; sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão. O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais. E quando o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados sempre que compatível com a finalidade do tratamento.

A lei chilena regula que o titular que autoriza o tratamento deve estar devidamente informado sobre o propósito do armazenamento de seus dados pessoais e sua possível transmissão. Os dados pessoais devem ser usados apenas para os fins para os quais foram recolhidos, a menos que provenham ou tenham sido coletados de fontes acessíveis ao público. Em qualquer caso, a informação deve ser precisa, atualizada conforme a situação real do titular.

A lei colombiana regula que o responsável pelo tratamento dos dados pessoais deve informar ao titular no momento da autorização: o tratamento para o qual seus dados pessoais e o propósito disso; a natureza facultativa da resposta às questões que são quando são sobre dados sensíveis ou sobre os dados de crianças e adolescentes; os direitos que o ajudam como titular; a identificação, endereço físico ou eletrônico e número de telefone do responsável pelo tratamento e todas essas informações devem ser registradas e estarem disponíveis para o titular, se ele necessitar de uma cópia.

A lei mexicana regula que o responsável é obrigado a informar ao titular, a informação que é coletado deles e para que fins, através do aviso de privacidade. O aviso de privacidade deve conter, pelo menos, as seguintes informações: a identidade e o endereço da pessoa responsável pela sua coleta; os fins do processamento de dados; as opções e significa que a pessoa responsável oferece aos detentores para limitar o uso ou divulgação dos dados; os meios para exercer os direitos de acesso, retificação, cancelamento ou oposição, de conformidade com as disposições desta Lei; quando aplicável, as transferências de dados que são feitas, e o procedimento e os meios pelos quais a pessoa encarregada comunicará aos

detentores de alterações ao aviso de privacidade, de acordo com as disposições desta lei. No caso de dados pessoais sensíveis, o aviso de privacidade deve declarar expressamente que trata deste tipo de dados.

A lei uruguaia regula que os titulares devem ser previamente informados de forma expressa e clara sobre a finalidade, a existência do arquivamento e a possibilidade que o titular tem de acessar, retificação e supressão de seus dados.

### 4.1.3 Princípios de Segurança de Dados

Em Segurança da Informação temos três princípios básicos: confidencialidade, disponibilidade e integridade. As leis abordam sobre estes princípios e ainda acrescentam outros que acharam relevantes ao tratamento dos dados pessoais. A lei argentina não trata sobre os princípios específicos sobre segurança de dados, mas regula que o responsável deve adotas medidas técnicas que garantam a segurança e a confidencialidade dos dados, de modo que se evite sua adulteração, perda, consulta ou tratamento não autorizado.

A lei boliviana não trata sobre os princípios específicos sobre segurança de dados, mas descreve princípios sobre o tratamento que são os seguintes: finalidade (o uso e o tratamento de dados pessoais devem obedecer a um propósito legítimo); veracidade (a informação sujeita a tratamento deve ser verdadeira, completa, precisa, atualizada, verificável, inteligível); transparência (o direito do proprietário de obter a qualquer momento e sem impedimento, as informações relacionadas à existência dos dados que lhe dizem respeito devem ser garantidas); segurança (os controles necessários para preservar a confidencialidade, integridade, disponibilidade, autenticidade, não repúdio e confiabilidade da informação devem ser implementados, fornecendo segurança aos registros, evitando sua falsificação, perda, uso e acesso não autorizado ou fraudulento); confidencialidade (todas as pessoas envolvidas no processamento de dados pessoais são obrigadas a garantir a confidencialidade das informações, mesmo após o término de seu vínculo com qualquer das atividades que compõem o tratamento).

O projeto de lei brasileiro trata os seguintes princípios: finalidade (pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular); adequação (pelo qual o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o

contexto do tratamento); necessidade (pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados); livre acesso (pelo qual deve ser garantida aos titulares consulta facilitada e gratuita sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais); qualidade dos dados (pelo qual devem ser garantidas aos titulares a exatidão, a clareza, relevância e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento); transparência (pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento); segurança (pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão); prevenção (pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e não discriminação (pelo qual o tratamento não pode ser realizado para fins discriminatórios).

A lei chilena não trata sobre princípios especificadamente como as demais leis. A lei colombiana trata os seguintes princípios: legalidade (atividade regulada que deve estar sujeito às disposições desta lei para desenvolvimento); finalidade (deve ter um propósito de acordo com a constituição e a lei); liberdade (o tratamento só pode ser exercido com consentimento prévio e expresso do titular); veracidade (a informação sujeita ao tratamento deve ser veraz, completa, precisa, atualizada, verificável e compreensível); transparência (é direto do titular, receber do responsável pelo tratamento informações sobre a existência de dados que lhe dizem respeito); acesso e circulação restrita (o tratamento está sujeito a limites decorrentes da natureza dos dados pessoais, as disposições desta lei e da constituição); segurança (a informação deve ser tratada com medidas técnicas, recursos humanos e administrativos que são necessários para garantir segurança dos registros evitando sua adulteração, perda, consulta, uso ou acesso não autorizado ou fraudulento); confidencialidade (deve-se garantir a confidencialidade de informações, mesmo após o fim de seu relacionamento, quando isso corresponde ao desenvolvimento das atividades autorizadas nesta lei e nos termos da lei).

A lei mexicana apenas cita os princípios utilizados, porém não explica cada um deles conforme as demais: “os responsáveis pelo tratamento de dados pessoais devem observar os princípios de legalidade, consentimento, informação, qualidade, propósito, lealdade, proporcionalidade e responsabilidade, previsto na lei”.

A lei uruguaia regula que as ações dos responsáveis pelas bases de dados, tanto públicas como privadas e, em geral, de todos aqueles que atuam em relação a dados pessoais de terceiros devem cumprir os seguintes princípios gerais: Legalidade; Veracidade; Finalidade; Prévio consentimento informado; Segurança de dados; Reserva e Responsabilidade.

### 4.1.4 Armazenamento de Dados

As leis também dispõem sobre o armazenamento dos dados pessoais e sobre seus formatos, no projeto de lei brasileiro apenas é citado que os dados pessoais devem ser armazenados em formato que favoreça o exercício do direito de acesso dos titulares. A lei argentina regula que o responsável deve manter as informações nas condições de segurança necessárias para evitar sua adulteração, perda, consulta, uso ou acesso não autorizado ou fraudulento. Deve ainda garantir e tomar as medidas necessárias para a manutenção da informação fornecida atualizada em seu banco de dados. Além de informar a estrutura básica dos arquivos, as transferências ou interconexões. A lei boliviana não dispõe sobre este assunto.

A lei chilena trata que todos têm o direito de exigir de quem é responsável por um banco de dados, que está envolvido no processamento de dados pessoais, sobre os dados relativos à pessoa, o objetivo do armazenamento dos mesmos e ainda pode solicitar a exclusão dos dados quando o armazenamento não é mais necessário. A lei colombiana regula que o responsável deve manter as informações nas condições de segurança necessárias para evitar sua adulteração, perda, consulta, uso ou acesso não autorizado ou fraudulento. Deve ainda garantir e tomar as medidas necessárias para a manutenção da informação fornecida atualizada em seu banco de dados. A lei mexicana regula que o responsável deve assegurar o cumprimento dos princípios da proteção de dados estabelecidos adotando as medidas necessárias para sua aplicação. Deve-se ainda realizar o processamento de dados pessoais mantendo medidas de segurança administrativa, técnica e física

que protejam os dados contra danos, perda, alteração, destruição ou uso não autorizado, acesso ou tratamento.

A lei uruguaia regula que qualquer banco de dados público ou privado deve ser registrado no Registro que o Corpo de Controle autoriza, de acordo com os critérios regulatórios que podem ser estabelecidos, dentre as quais o seguinte aparecerá necessariamente: Identificação do banco de dados e a pessoa responsável por ele; Natureza dos dados pessoais contidos; Procedimentos para obter e processar os dados; Medidas de segurança e descrição técnica da base de dados; Proteção de dados pessoais e exercício de direitos; Destino dos dados e pessoas físicas ou jurídicas a que podem ser transmitidos; Tempo de conservação dos dados; Forma e condições em que as pessoas podem acessar os dados que lhes são encaminhados e os procedimentos a serem realizados para corrigir ou atualizar os dados.

### 4.1.5 Modificação de Dados

A alteração de dados também é regulamentada pelas leis, porém não abordada por todas, como no caso da lei boliviana. A lei argentina regula que o titular dos dados pessoais tem o direito de obter a correção de dados incompletos, inexatos ou desatualizados quando correspondam a dados que estejam armazenados em banco de dados. O projeto de lei brasileiro regula que o titular dos dados pessoais tem o direito de obter a correção de dados incompletos, inexatos ou desatualizados e no caso de alteração de informação, o responsável deverá comunicar ao titular as informações de contato atualizadas.

A lei chilena regula que caso os dados pessoais sejam errôneos, impreciso, equívoco ou incompleto, e isso está comprovado, terá o direito de ser modificado. O direito das pessoas às informações, modificações, cancelamentos ou bloqueios de seus dados pessoais não podem ser limitados por qualquer meio ato ou convenção.

A lei colombiana regula que o responsável deve atualizar a informação, comunicando o titular sobre os dados que anteriormente foram fornecidos e as medidas tomadas para a manutenção da informação.

A lei mexicana trata que nos casos de pedidos de retificação de dados pessoais, o proprietário deve indicar as modificações a serem feitas e fornecer a documentação que suporte seu pedido. O responsável pode negar o acesso a dados

pessoais ou a realizar a retificação ou cancelamento ou concessão da oposição ao seu tratamento, nos seguintes casos: quando o requerente não é o proprietário dos dados pessoais, ou o representante legal não é devidamente credenciado para ele; quando no seu banco de dados, os dados pessoais do candidato não são encontrados; quando os direitos de um terceiro estão feridos; quando há um impedimento legal, ou a resolução de uma autoridade competente, que restringe acesso a dados pessoais, ou não permitir a retificação, cancelamento ou oposição dos mesmos, e quando a retificação, cancelamento ou oposição foi feita anteriormente.

A lei uruguaia regula que toda pessoa deve ter o direito de levar a cabo uma ação judicial efetiva para conhecer os dados referentes à sua pessoa e seu propósito e uso, que estão contidos em bancos de dados públicos ou privados e em caso de erro, falsidade, proibição de tratamento, discriminação ou desatualizado para exigir a sua retificação, inclusão, supressão ou o que corresponda.

### 4.1.6 Anonimização de Dados

Apenas o projeto de lei brasileiro traz este termo e contempla dados anonimizados nas disposições. Conforme o PL, anonimização é qualquer procedimento por meio do qual um dado deixa de poder ser associado, direta ou indiretamente, a um indivíduo. Estes dados serão considerados dados pessoais para os fins desta lei quando o processo de anonimização ao qual foram submetidos for revertido. O compartilhamento e o uso que se faz de dados anonimizados deve ser objeto de publicidade e de transparência, sem prejuízo do órgão competente poder solicitar ao responsável relatório de impacto à privacidade referente aos riscos de reversão do processo de anonimização e demais aspectos de seu tratamento. O órgão competente poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de sua segurança.

### 4.1.7 Bloqueio/Eliminação de Dados

O bloqueio ou a eliminação dos dados também está prevista em lei, apenas as leis argentina e boliviana não contemplam regulamentação específica para isso. O projeto de lei brasileiro define que eliminação é a “exclusão definitiva de dado ou

de conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado". O titular pode solicitar a eliminação, a qualquer momento, de dados pessoais com cujo tratamento o titular tenha consentido. Os dados pessoais serão eliminados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades: cumprimento de obrigação legal do responsável; pesquisa histórica, científica ou estatística, garantida, quando possível, a anonimização dos dados pessoais; ou transferência a terceiros, desde que respeitados os requisitos de tratamento de dados dispostos na lei.

A lei chilena regula que se os dados pessoais foram cancelados ou modificados pelo responsável é necessário que previamente sejam comunicados aos titulares dos dados sobre a operação realizada. Se não fosse possível determinar o número de pessoas que foram notificadas, deve-se notificar via nota de conhecimento geral para aqueles que usam as informações no banco de dados. O direito das pessoas às informações, modificações, cancelamentos ou bloqueios de seus dados pessoais não podem ser limitados por qualquer meio ato ou convenção.

A lei colombiana regula que o titular que consideram que seus dados contidos em um banco de dados devem ser corrigidos, atualizados ou excluídos, devem apresentar um pedido perante o responsável pelo tratamento que será processado de acordo com as regras estabelecidas em lei.

A lei mexicana regula que a identificação e conservação de dados pessoais, deve ser mantido até o prazo de prescrição legal ou contratual destes. Durante este período, os dados pessoais não podem ser processados e, uma vez que este procederá ao seu cancelamento no banco de dados correspondente aos dados pessoais resultará em um período de bloqueio. O período de bloqueio será equivalente ao termo de prescrição das ações derivadas do relacionamento legal que funda o tratamento nos termos de a lei aplicável na matéria. A pessoa responsável pode mantê-los exclusivamente para os fins decorrentes do tratamento. Uma vez que os dados foram cancelados, aviso será dado ao seu proprietário.

A lei uruguaia regula que a eliminação ou supressão de dados pessoais não é aplicável, exceto nos casos de: prejuízo dos direitos e interesses legítimos de terceiros; erro notório ou falsidade ou violação do que é estabelecido por uma obrigação legal.

### 4.1.8 Transferência Internacional de Dados

Ponto importante e de maior interesse para organização X, a transferência internacional de dados se refere à transferência de dados pessoais para outros países que não é autorizada em nenhuma das leis, porém existem casos em que se é permitido essa operação seguindo algumas regras. A lei argentina regula que é proibida a transferência de dados pessoais de qualquer tipo com países que não proporcionem níveis de proteção adequados. Porém a proibição não regerá nas seguintes situações: colaboração judicial internacional; transferências bancárias; por meio de tratados internacionais ou que tenha o objetivo de cooperação internacional entre organismos de inteligência para a luta sobre o crime organizado, o terrorismo e o narcotráfico. O projeto de lei brasileiro regula que somente é permitida a transferência nos seguintes casos: para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao do projeto de lei; quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional; quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros; quando o órgão competente autorizar a transferência; quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público; quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos. Se a transferência for autorizada em qualquer uma das situações acima, será avaliado o nível de proteção de dados do país pelo órgão competente, que levará em conta: as normas gerais e setoriais da legislação em vigor no país de destino; a natureza dos dados; princípios gerais de proteção de dados pessoais previstos nesta lei; adoção de medidas de segurança previstas em regulamento. O órgão competente poderá ainda elaborar cláusulas contratuais padrão que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular. Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou

conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

A lei colombiana trata a transferência de dados pessoais como proibição se o país de destino não fornecer níveis adequados de proteção de dados, entende-se adequado quando cumpre os padrões estabelecidos pela Superintendência de Indústria e Comércio da Colômbia sobre o assunto, que em nenhum caso pode ser inferior a que a Lei exige. Esta proibição não se aplica quando se lida com situações como: informações sobre as quais o titular concedeu sua autorização para a transferência; transferências necessárias para a execução de um contrato entre o titular e responsável pelo tratamento, ou para a execução de medidas contratuais, desde com a autorização do titular; transferências legalmente exigidas para a salvaguarda do interesse público, ou para o reconhecimento, exercício ou defesa de um direito em um processo judicial.

A lei mexicana regula que quando a pessoa responsável pretende transferir os dados pessoais para terceiros nacionais ou estrangeiros, além da pessoa responsável, deve comunicar o aviso de privacidade e os propósitos para aqueles que o titular submeteu seu tratamento. O processamento dos dados será feito a partir do acordo realizado no aviso de privacidade, que conterá uma cláusula indicando se o titular aceitará ou não a transferência de seus dados, desta forma, o terceiro assumirá as mesmas obrigações que correspondem à pessoa responsável transferiu os dados.

A lei uruguaia regula que é proibida a transferência de dados pessoais de qualquer tipo com países que não proporcionem níveis de proteção adequados. Porém a proibição não regerá nas seguintes situações: colaboração judicial internacional; transferências bancárias; por meio de tratados internacionais ou que tenha o objetivo de cooperação internacional entre organismos de inteligência para a luta sobre o crime organizado, o terrorismo e o narcotráfico.

### 4.1.9 Fiscalização

Para que a lei entre em vigor, há fiscalização por meio de órgãos indicados pelas leis. A lei boliviana não contempla um órgão específico para a fiscalização do tratamento de dados pessoais. A lei argentina regula que o órgão de controle deverá

realizar todas as ações para garantir os direitos e deveres presentes na legislação, quem descumprir deverá responder às sanções administrativas e penais de acordo com a constituição do país. O projeto de lei brasileiro regula que as infrações realizadas por pessoas jurídicas de direito privado às normas previstas ficam sujeitas às sanções administrativas aplicáveis pelo órgão competente e o Conselho Nacional de Proteção de Dados e da Privacidade que contará com quinze representantes titulares e quinze suplentes designados pelo Ministro de Estado da Justiça. Eles são designados para zelar pela implementação e fiscalização da futura lei.

A lei chilena regula que a o responsável pelos dados pessoais não seguir as disposições nela presentes, deverá compensar o dano moral causado pelo tratamento inadequado dos dados, de acordo com o que é exigido pelo titular ou, conforme o caso, ordenado pelo tribunal. O juiz tomará todos os arranjos que considera conveniente fazer proteção efetiva dos direitos que a lei estabelece e o montante da compensação será estabelecido prudencialmente pelo juiz, considerando as circunstâncias do caso e a gravidade dos fatos.

A lei colombiana regula que a Superintendência de Indústria e Comércio, através de uma Delegação para a Proteção de Dados Pessoais, exercerá vigilância para garantir que no processamento de dados os princípios, direitos, garantias e procedimentos são respeitados previsto em lei.

A lei uruguaia não dispõe de um órgão fiscalizador, porém quem descumprir seu regulamento responderá às sanções descritas em lei.

## 4.2 PROPOSTA DE DIRETRIZES PARA O TRATAMENTO DE DADOS PESSOAIS

As diretrizes foram consideradas para atender a maior parte de tópicos acima citados, pela atuação na América Latina (Colômbia/Argentina) da empresa X. Principalmente pela transferência de dados constante, já que a matriz é brasileira e as informações das filiais são administradas pela mesma. A empresa X e suas filiais são entidades comprometidas com a proteção da privacidade e de toda informação que possa ser associada a pessoas, determinados ou determináveis ("Dados Pessoais"), aos quais têm acesso em suas atividades comerciais.

As diretrizes propostas estão disponíveis no APÊNDICE A e têm suas seções detalhadas a seguir.

### 4.2.1 Definição

Foi definido para que a empresa X se propôs a fazer uma Política específica para o tratamento de dados pessoais e que se aplica aos parceiros de negócios, fornecedores, clientes, funcionários, funcionários, contratados e, em geral, a qualquer pessoa cujos dados pessoais sejam ou serão ser tratados pela empresa.

### 4.2.2 Princípios de Segurança de Dados

Em Segurança da Informação temos três princípios básicos: confidencialidade, disponibilidade e integridade. É importante deixar claro quais princípios a empresa segue sobre o tratamento dos dados pessoais, ao se fiscalizar saberá exatamente a quais premissas o tratamento se baseia. Por esse motivo, utilizou-se dos princípios descritos na lei colombiana, transcrevendo na própria política definindo o que será seguido pela empresa X.

### 4.2.3 Tipos de Dados e Formas que se Coletam

A organização X recebe, coleta, usa, administra, analisa, segmenta, indexa, transmite, transfere, armazena e, geralmente, processa dados pessoais, como os de identificação (nome, documento de identificação, gênero, data de nascimento), de contato (telefone, e-mail, endereço), de visitas e informações financeiras, comportamento do consumidor, entre outros, como responsável pelo processamento de Dados Pessoais, informações que podem ser obtidas durante o curso e para o desempenho de suas atividades comerciais.

### 4.2.4 Autorização para o Tratamento

Todo tratamento deve estar precedido pela obtenção da autorização prévia, expressa e informada dos titulares, conforme as Leis da América Latina e Projeto de Lei do Brasil. Para isso a empresa X, antes da coleta de dados pessoais, também retêm evidências do consentimento prévio, expresso e informado concedido pelo

titular para consultas futuras. A autorização dos titulares pode ser expressa por escrito ou por qualquer meio que possa estar sujeito a consulta adicional.

### 4.2.5 Finalidades do Tratamento

De acordo com a organização X e em conformidade com as diretrizes das Leis, foram definidas algumas finalidades, disponibilizações e destino dos dados pessoais tratados pela mesma, como: envio de notícias, convite para eventos da organização, campanhas de publicidade e mercado, pesquisas de satisfação, estudo de crédito, fornecimento de produtos e serviços, informações de pedidos, cumprimento de obrigações legais de informação às autoridades que assim o exijam, entre outras. Disponível no apêndice dessa pesquisa, a Política completa para eventuais consultas.

### 4.2.6 Direitos dos Titulares

Os dados pessoais são utilizados para fins definidos e descritos na política, os responsáveis da empresa X em nenhum caso estão autorizados a realizar tratamento para fins diferentes dos descritos na mesma. Definiu-se os dados que são coletados e os meios se utiliza para isso, no exercício de atividades realizadas por meio de vínculos comerciais, contratuais, trabalhistas ou outros com seus usuários, clientes, fornecedores, contratados, funcionários ou o público em geral, e canais não presenciais como o site e o telefone.

Os titulares têm o direito de atualizar seus dados pessoais que retém nas bases de dados da empresa X para manter sua integridade e veracidade. É direito do titular também solicitar a exclusão de seus dados pessoais de bancos de dados da empresa X, desde que não haja nenhuma obrigação legal ou obrigação de natureza contratual do titular com a empresa X, de acordo com o qual o titular não tem o direito de solicitar a exclusão de seus dados pessoais. O pedido de exclusão da informação e a revogação da autorização não serão realizados quando o titular tiver um dever legal ou contratual com a empresa X.

### 4.2.7 Área de Proteção de Dados Pessoais

A empresa X tem uma unidade encarregada da recepção e atenção das petições, queixas e reclamações relacionadas aos Dados Pessoais: Serviço ao Cliente. Dentro desta unidade, o Serviço ao Cliente processará consultas e reivindicações relativas a Dados Pessoais de acordo com a lei, procedimentos internos e esta política.

### 4.2.8 Vigência

A Política entrará em vigor a partir de Janeiro de 2018, para que possa passar pelo processo de transição e conhecimento de todos os colaboradores. Os dados pessoais armazenados, utilizados ou transmitidos permanecerão nos bancos de dados da empresa X, com base no critério da temporalidade, desde que seja necessário cumprir os propósitos mencionados nesta política, para os quais foram coletados.

### 4.2.9 Outras Disposições

Nessa seção foram descritos as exceções ou pontos de atenção sobre a política, como: a transferência de dados que estará coberta por um contrato firmado pela matriz com suas filiais em que os dados devem ser tratados e mantidos pela mesma, bem como na autorização do titular esse contrato é firmado também com o conhecimento do mesmo; não pretende coletar dados pessoais confidenciais de crianças ou menores, pois estes precisam de tratamento específico conforme as Leis; e sobre que a Política pode ser modificada e deve fazer parte dos contratos celebrados pela mesma, quando aplicável. Porém qualquer modificação deverá ser comunicada antecipadamente aos Titulares por meio de mecanismos eficientes.

# 5 CONSIDERAÇÕES FINAIS

A proteção da privacidade e dos dados pessoais cada vez mais ganha importância nos dias atuais, o viver em sociedade e a tutela do direito constantemente é desafiada por essas novas questões que se demonstram atuais e efetivas na sociedade da informação. Uma vez que o tema já é realidade em países da América Latina, a tendência é que as empresas brasileiras se preocupem mais com este assunto. As leis existentes no Brasil falham na tarefa de proteger os dados pessoais, segundo Costa (2015) é preciso garantir a disciplina dessa temática de forma democrática, com a participação do usuário, o maior interessado no regramento que dará as diretivas para tratamento de seus dados pessoais. Faz-se necessário disciplinar as questões omissas nas normas existentes, bem como modificar procedimentos que, a par de cumprir a legislação, falham na proteção real de dados pessoais. Um exemplo é o consentimento. A partir do contexto acima, a questão de pesquisa se baseia em: quais fatores devem ser contemplados na adoção de práticas específicas para tratamento de dados pessoais de colaboradores, clientes e fornecedores?

A partir dessa questão a pesquisa se pautou em buscar conceitos base que pudessem auxiliar a tratar deste assunto. Para isso, foram utilizados conceitos de Gestão da Informação (GI) que dentro das organizações é utilizada para gerir os recursos internos quantos os externos. A Segurança da Informação (SI) foi discutida como estratégia de processos de GI, ao oferecer às organizações um maior controle. Além da preocupação com a segurança de informações gerais, as organizações devem proteger com maior atenção os dados pessoais coletados de clientes, funcionários e outros cadastrados em seus bancos de dados. Foram analisadas as legislações pertinentes ao Brasil e uma breve incitação sobre este assunto mundialmente, a partir da necessidade da organização X, foram analisadas em conjunto as leis que regem os países da América Latina. E após o levantamento de seus pontos mais importantes, foram propostas diretrizes para o tratamento de dados pessoais, construída a partir da necessidade da organização objeto de estudo.

## 5.1 LIMITAÇÕES DA PESQUISA

Dentre as limitações apresentadas pela pesquisa, é possível destacar que não foram analisadas leis, ou mesmo projetos de leis, fora do continente latino-americano, uma vez que se privilegiou a área de atuação da organização estudada. Além disso, não foram consideradas soluções adotadas por outras organizações, públicas ou privadas, que enfrentam a mesma necessidade de proteção de dados pessoais e/ou transferência internacional de dados. Bem como, outras pesquisas que foram realizadas sobre o tema, pela limitação do tempo desta pesquisa.

Por fim, a política proposta não foi colocada em prática para verificar seus reais benefícios junto à organização. Uma aplicação prática da política poderá apresentar necessidades não contempladas nesta proposta. De qualquer maneira, seu conteúdo determina que a mesma possa ser modificada em caso de necessidade.

## 5.2 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Diante das limitações apresentadas, destaca-se entre as sugestões para trabalhos futuros a análise de leis e/ou projetos de leis de outros país e continentes. Assim, a partir de um contexto cultural mais abrangente podem-se levantar tópicos não contemplados neste trabalho o que acarretará em modificações na política proposta que garantirá sua aplicação em organizações que atuam além da América Latina.

Como outra fonte de comparação, recomenda-se também, a adoção de um *benchmarking* em organizações públicas e privadas que apresentam as mesmas necessidades da Organização X relativas ao tratamento de dados pessoais. Por fim, será interessante verificar quais os resultados práticos gerados a partir da adoção da política proposta.

## 5.3 CONTRIBUIÇÕES DA PESQUISA

A Segurança da Informação é uma área muito importante dentro Gestão da Informação. Uma vez que toda empresa possui clientes e parcerias, manter seguras as informações de terceiros vai além de simplesmente evitar o extravio destas.

Deste modo, a empresa deve ter o compromisso e a ética em resguardar os dados que estão em seu poder e saber trata-las adequadamente. A pesquisa contribuiu para que as organizações multinacionais e também as organizações de atuação nacional saibam como estudar a viabilidade da aplicação de políticas e procedimentos sobre os dados pessoais e suas obrigações ao tratar este tipo de dado de forma com que estejam de acordo com as Leis regentes. Além disso, fornece uma proposta de diretrizes para o tratamento de dados pessoais que pode ser adotada em organizações que atuam no Brasil ou mesmo na América Latina, uma vez que contempla as principais exigências das leis vigentes no continente.

## REFERÊNCIAS

ABREU, Dimitri. 2001. Melhores Práticas para Classificar as Informações. **Módulo e-Security Magazine**. São Paulo. Disponível em: <www.modulo.com.br>. Acesso em: 14 maio 2017.

ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. 2002. **Segurança no Desenvolvimento de Software** – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Editora Campus. Rio de Janeiro.

ANTHONY, Robert Newton. **Planning and Control Systems:** A framework for analysis. Cambridge: Harvard University Press, 1965, 180p.

ARGENTINA. Ley nº 25.326 de 4 de Outubro de 2000. Protección de los Datos Personales. Presidencia de la nación. Buenos Aires, 2000. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>. Acesso em: 11 dez. 2017.

BEAL, Adriana. **Gestão estratégica da informação**: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações – 3. Reimpr. – São Paulo: Atlas, 2008.

BERBERT, Lucia. **Especialistas defendem criação de autoridade garantidora de proteção de dados pessoais.** 2017. Disponível em: <http://www.mobiletime.com.br/07/06/2017/especialistas-defendem-criacao-de-autoridade-garantidora-de-protecao-de-dados-pessoais/471642/news.aspx?__akacao=4239374&__akcnt=69c8e8ee&__akvkey=1837&utm_source=akna&utm_medium=email&utm_campaign=MOBILE+TIME+News+-+07/06/2017+22:47>. Acesso em: 11 dez. 2017.

BOLÍVIA. Decreto Nº 1.793, de 13 de novembro de 2013. Reglamento para el desarrolo de tecnologías de informacuión y comunicación. **Secretaria General de la Presidencia de la Republica**. La Paz, 2013. Disponível em: <http://www.wipo.int/edocs/lexdocs/laws/es/bo/bo058es.pdf> Acesso em: 12 ago. 2017.

BOUCA, Carla. **O que é a EU GDPR por que ela é aplicável para todo o mundo?** Disponível em: <https://advisera.com/27001academy/pt-br/blog/2016/10/07/o-que-e-a-eu-gdpr-por-que-ela-e-aplicavel-para-todo-o-mundo/> Acesso em: 23 de Outubro de 2017.

BRAGA, Ascenção. **A gestão da informação**. Millenium, n. 19, jun. 2000.

BRASIL. APL 5276/2016, de 13 de maio de 2016. Anteprojeto de Lei de Proteção de Dados Pessoais. **Poder Executivo do Brasil.** Brasília, DF, 2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 12 ago. 2017.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da república Federativa do Brasil**. Brasília, DF, 2014. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 11 agosto 2017.

BRASIL. PORTAL BRASIL. **Governo quer maior proteção para dados pessoais no País.** 2015. Disponível em: <http://www.brasil.gov.br/defesa-e-seguranca/2015/11/governo-quer-maior-seguranca-para-dados-pessoais-da-populacao>. Acesso em: 17 jul. 2017.

BRASIL. Projeto que protege dados pessoais passa na CCT, mas ainda vai a três comissões. **Agência Senado**, 2015. Disponível em: < https://www12.senado.leg.br/noticias/materias/2015/10/13/marco-regulatorio-para-protecao-de-dados-pessoais-e-aprovado-pela-cct-e-segue-para-tres-outras-comissoes>. Acesso em: 17 jul. 2017.

BRASIL. Marco regulatório para proteção de dados pessoais é aprovado pela CCT e segue para três outras comissões. **Senado**, 2015. Disponível em: < https://senado.jusbrasil.com.br/noticias/242116242/marco-regulatorio-para-protecao-de-dados-pessoais-e-aprovado-pela-cct-e-segue-para-tres-outras-comissoes>. Acesso em: 11 dez. 2017.

CAMPOS, Claudinei José Gomes. Método de análise de conteúdo: ferramenta para a análise de dados qualitativos no campo da saúde. **Rev. bras. enferm.** Brasília, v. 57, n. 5, p. 611-614, out 2004. Disponível em: <http://dx.doi.org/10.1590/S0034-71672004000500019>. Acesso em: 21 jun. 2017.

CHILE. Lei nº 19.628, de 28 de agosto de 1999. Protección de Datos de Carácter Personal. **Ministerio Secretaria General de la Presidencia.** Santiago, 1999. Disponível em: <https://www.leychile.cl/Navegar?idNorma=141599>. Acesso em: 12 ago. 2017.

CHOO C. Wei. **A organização do conhecimento**. São Paulo: SENAC, 2003.

COLÔMBIA. Lei nº 1.581, de 18 de outubro de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. **Diario Oficial de la Republica de Colombia**. Bogotá, DC, 2012. Disponível em: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>. Acesso em 12 ago. 2017.

COSTA, Thabata Filizola. **A importância de uma Lei Geral de Proteção de Dados Pessoais.** 2015. Disponível em: <https://thabatafc.jusbrasil.com.br/artigos/346208302/a-importancia-de-uma-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 11 dez. 2017.

DANTAS, M. **Segurança da Informação**: uma abordagem focada em gestão de riscos. 1 ed. Olinda: Livro rápido, 2011.

DAVENPORT, Thomas H.; PRUSAK, Laurence. **Ecologia da informação**: por que só a tecnologia não basta para o sucesso na era da informação. Futura, 1995.

ESPANHA. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado. Madrid, 1999. Disponível em:

<https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>. Acesso em: 12 ago. 2017.

FAUSTINO, André. A proteção de dados pessoais no Brasil: Breve histórico do direito comparado até a atual realidade brasileira. In: **Âmbito Jurídico**, Rio Grande, XIX, n. 154, nov 2016. Disponível em: <http://ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=18241>. Acesso em 11 dez. 2017.

FERREIRA, Tereza Evâny de Lima Renôr; PERUCCHI, Valmira. Gestão e o fluxo da informação nas organizações: um ensaio a partir da percepção de autores contemporâneos. **Revista ACB**, [S.l.], v. 16, n. 2, p. 446-463, dez. 2011. Disponível em: <https://revista.acbsc.org.br/racb/article/view/781>. Acesso em: 10 dez. 2017.

GALVÃO, Thiago. A Importância da Proteção das Informações Pessoais. **TI especialistas**, nov. 2010. Disponível em: <https://www.tiespecialistas.com.br/2010/11/a-importancia-da-protecao-das-informacoes-pessoais/>. Acesso em: 17 jun. 2017.

LAUREANO, Marcos Aurelio Pchek; MORAES, Paulo Eduardo Sobreira. Segurança como estratégia de gestão da informação. **Revista Economia & Tecnologia**, v.8, n.3, p.38-44, 2005. Disponivel em: < http://www.mlaureano.org/projects/seguranca/economia_tecnologia_seguranca.pdf>. Acesso em: 17 jun. 2017

MARCIANO, João Luiz; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. **Ci. Inf.**, Brasília, v. 35, n. 3, p. 89-98, Dez. 2006. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652006000300009&lng=en&nrm=iso>. Acesso em: 11 Dez. 2017.

MCGEE, James V.; PRUSAK, Laurence. **Gerenciamento estratégico de Informação:** aumente a competitividade e a eficiência da sua empresa utilizando a informação como uma ferramenta estratégica – Rio de Janeiro: Campus, 1994.

MÉXICO. Lei LFPDPPP, de 05 de julho de 2010. Protección de datos personales en posesión de los particulares. **Diario Oficial de la Federación de Mexico**. México, DF, 2010. Disponível em: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>. Acesso em: 12 ago. 2017.

MICHAELIS. **Dicionário online Michaelis**, 13 nov. 2017. Disponível em < http://michaelis.uol.com.br/moderno-portugues>. Acesso em 13 nov. 2017.

REZENDE, Denis Alcides e ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. Editora Atlas. São Paulo, 2000.

ROUSE, Margaret. **Personally Identifiable Information (PII)**. 2014. Disponível em: <http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information>. Acesso em: 14 maio 2017.

SÁ, Antonio Lopes de. 2001. **Ética profissional.** São Paulo: Atlas.

SILVA, Edna Lúcia da; MENEZES, Estera Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. Florianópolis, UFSC. Disponível em: <https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf>. Acesso em: 14 maio 2017.

URUGUAI. Ley Nº 18.331 de 18 de agosto de 2008. Protección de Datos Personales y Acción de “Habeas Data”. **República Oriental del Uruguay.** Montevideo, 2008. Disponível em: <https://legislativo.parlamento.gub.uy/temporales/leytemp4999828.htm>. Acesso em: 11 dez. 2017.

VITAL, Luciane Paula; FLORIANI, Vivian Mengarda; VARVAKIS, Gregório. Gerenciamento do fluxo de informação como suporte ao processo de tomada de decisão: revisão. **Informação & Informação**, [S.l.], v. 15, n. 1, p. 85-103, jul. 2010. Disponível em: <http://www.uel.br/revistas/uel/index.php/informacao/article/view/5335>. Acesso em: 11 dez. 2017.

## APÊNDICE A - DIRETRIZES PARA O TRATAMENTO DE DADOS PESSOAIS

A organização X e suas filiais são entidades comprometidas com a proteção da privacidade e de toda informação que possa ser associada a pessoas, determinados ou determináveis ("Dados Pessoais"), aos quais têm acesso em suas atividades comerciais. A organização X recebe, coleta, usa, administra, analisa, segmenta, indexa, transmite, transfere, armazena e, geralmente, utiliza dados pessoais, como os de identificação (nome, documento de identificação, gênero, data de nascimento), de contato (telefone, e-mail, endereço), de visitas e informações financeiras, comportamento do consumidor, entre outros, como responsável pelo processamento de Dados Pessoais, informações que podem ser obtidas durante o curso e para o desempenho de suas atividades comerciais.

As diretrizes descritas a seguir são dirigidas aos parceiros de negócios, fornecedores, clientes, funcionários, funcionários, contratados e, em geral, a qualquer pessoa cujos dados pessoais sejam ou serão ser tratado pela empresa X. Se aplicará a todo tratamento realizado dentro dos territórios das empresas e suas filiais.

### 1 DEFINIÇÕES

Para os fins deste documento devem ser considerados:

- “Tratamento”: Qualquer operação ou conjunto de operações sobre dados pessoais, tais como a coleta, armazenamento, uso, circulação, transferência e distribuição.
- “Dado Sensível”: Os dados sensíveis são aqueles que afetam a privacidade do Titular ou cujo abuso pode levar a discriminação, como aqueles que revelam origem racial ou étnica, orientação política, crenças religiosas ou filosóficas, adesão a sindicatos, organizações sociais, de direitos humanos ou que promova os interesses de qualquer partido político ou que garantam os direitos e garantias dos partidos políticos de oposição, bem como os dados relacionados à saúde, vida sexual e dados biométricos.

## 2 PRINCÍPIOS PARA O TRATAMENTO DOS DADOS PESSOAIS

- Princípio da legalidade em matéria de tratamento de dados: atividade regulada que deve estar sujeita às disposições aqui descritas para seu desenvolvimento;
- Princípio de finalidade: O tratamento deve ter um propósito de acordo com as finalidades descritas neste documento, que deve ser informado ao titular;
- Princípio de liberdade: O tratamento só pode ser exercido com consentimento prévio e expresso do titular;
- Princípio de veracidade: A informação sujeita ao tratamento deve ser veraz, completa, precisa, atualizada, verificável e compreensível. É proibida a utilização de dados pessoais parciais, incompletos, fracionados ou enganosos;
- Princípio de transparência: É direto do titular, receber do responsável pelo tratamento, a qualquer momento e sem restrições, informações sobre a existência de dados que lhe dizem respeito;
- Princípio de acesso e circulação restrita: O tratamento está sujeito a limites decorrentes da natureza dos dados pessoais, as disposições desta lei e da Constituição;
- Princípio de segurança: A informação sujeita ao tratamento referido neste documento, deve ser tratada com medidas técnicas, recursos humanos e administrativos que são necessários para garantir segurança dos registros evitando sua adulteração, perda, consulta, uso ou acesso não autorizado ou fraudulento;
- Princípio de confidencialidade: Todas as pessoas envolvidas em processamento de dados pessoais são responsáveis em garantir a confidencialidade de informações, mesmo após o fim de seu relacionamento com algumas das tarefas que inclui o tratamento, podendo apenas fornecer dados pessoais, quando isso corresponde ao desenvolvimento das atividades autorizadas neste documento.

## 3 TIPOS DE DADOS PESSOAIS E FORMAS EM QUE SE COLETAM

A empresa X coleta dados pessoais (i) no exercício de atividades realizadas por meio de vínculos comerciais, contratuais, trabalhistas ou outros com seus usuários, clientes, fornecedores, contratados, funcionários ou o público em geral, e (ii) canais não presenciais não presenciais como o site e o telefone. Os dados pessoais são armazenados em aplicativos ou softwares adequadamente licenciados.

Os seguintes tipos de dados pessoais são sobre os quais a empresa X realiza tratamento:

- Nome; Número de documento de identificação; Endereço; Telefone; E-mail; e informações de contato.
- Nacionalidade; Data de nascimento; Sexo e Estado civil.
- Profissão; Empresa; Cargo e Dados de contato.
- Informações são enviadas ou consultadas através de bancos de dados de redes sociais, entre outros meios, onde foi incluído dados pessoais.
- Endereço IP e tipo de navegador, quando obtidos por meios eletrônicos.
- Informação financeira.
- Qualquer informação necessária para pedidos especiais.
- Informações que fornecidas em relação às preferências comerciais ou no curso da participação em pesquisas, concursos ou ofertas promocionais.
- Imagens, fotografias e impressões digitais.
- Dados pessoais considerados sensíveis.

## 4 AUTORIZAÇÃO PARA O TRATAMENTO

Todo tratamento deve estar precedido pela obtenção da autorização prévia, expressa e informada dos titulares. Para isso a empresa X, antes da coleta de Dados Pessoais, também retêm evidências do consentimento prévio, expresso e informado concedido pelo Titular para consultas futuras. A autorização dos titulares pode ser expressa por escrito ou por qualquer meio que possa estar sujeito a consulta adicional.

## 5 FINALIDADES DO TRATAMENTO

Os dados pessoais são utilizados para os seguintes fins abaixo, os colaboradores responsáveis da empresa X em nenhum caso estarão autorizados a realizar tratamento para fins diferentes dos descritos aqui:

- Enviar informações sobre notícias, mudanças nos produtos ou serviços, informações promocionais, publicitárias de marketing e administrativas dos produtos ou serviços da empresa X, bem como suas atividades e eventos.
- Informação básica no processo de entrega de pedidos.
- Para consultar e atualizar dados pessoais, em qualquer momento, com o fim de manter atualizadas as informações.
- Convite para eventos realizados pela empresa X.
- Realizar campanhas de publicidade e mercado.
- Realizar pesquisas de satisfação e avaliação de qualidade de produtos e serviços.
- Preparar estudos de mercado para estabelecer preferências do consumidor.
- Realizar estudos de crédito, cobrança, risco de crédito ou riscos de qualquer tipo.
- Promoção de acordos comerciais, eventos ou programas institucionais diretamente ou em parceria com terceiros.
- Fornecer os nossos produtos e serviços necessários diretamente ou através de terceiros.
- Verificação de dados através da consulta de bancos de dados de risco públicos ou centrais.
- Enviar informações sobre atividades desenvolvidas pela empresa X ou enviar informações que sejam consideradas de interesse por diferentes meios.
- Cumprimento das obrigações legais de informação às entidades administrativas, bem como às autoridades competentes que assim o exijam.
- Compartilhar com terceiros que prestam serviço para a empresa X e que, para o cumprimento de suas funções, tenham acesso até certo ponto à

informação, como prestadores de serviços de e-mail, agências de publicidade, call centers e bancos. A empresa X afirma que usará sua melhor diligência em favor de que esses terceiros mantenham a confidencialidade das informações a que têm acesso, tudo isso regulado por acordos de confidencialidade assinados com eles.

- Executar obrigações decorrentes de contratos comerciais e trabalhistas em que a empresa X é uma das partes.
- Dar suporte aos processos de auditoria da empresa X.
- Confirmar compras de produtos efetuadas via web.
- Qualquer outro propósito que possa resultar no contrato ou na relação comercial entre a empresa X e o titular.

## 6 DIREITOS DOS TITULARES

Os titulares possuem os seguintes direitos:

- Atualização: Atualizar dados pessoais que retém nas bases de dados da empresa X para manter sua integridade e veracidade.
- Conhecimento e acesso: O titular poderá acessar seus dados gratuitamente, mediante solicitação prévia, pelo menos uma vez por mês.
- Prova: Solicitar prova de autorização concedida à empresa X, a menos que a lei indique que tal autorização não é necessária.
- Queixa: Submeter reclamações à Superintendência de Indústria e Comércio ou órgão responsável pela fiscalização por violações da lei quando o requisito processual foi esgotado e apelar em primeira instância para empresa X.
- Correção: Corrigir as informações e os Dados Pessoais que estão sob o controle da empresa X.
- Revogação: Solicitar de revogação da autorização, desde que não haja obrigação legal ou obrigação contratual do titular com a empresa X.
- Exclusão: Solicitar a exclusão de seus dados pessoais de bancos de dados da empresa X, desde que não haja nenhuma obrigação legal ou obrigação de natureza contratual do titular com a empresa X, de acordo com o qual o titular não tem o direito de solicitar a exclusão de seus dados pessoais.

Os titulares podem exercer os seus direitos e cumprir os procedimentos estabelecidos neste documento entrando em contato com a empresa X através dos canais de comunicação disponíveis. A empresa X será responsável por responder a pedidos ou reclamações de acordo com as regras para a proteção de Dados Pessoais na América Latina e nos termos estabelecidos neste documento. Qualquer solicitação a respeito disso deverá incluir as seguintes informações:

- Dados de identificação do titular e documentos comprobatórios.
- A descrição dos fatos que originaram a reivindicação.
- O endereço para notificação ou resposta.
- Documentos que se deseja firmar.
- Conteúdo e justificativa da solicitação.

O prazo máximo para atender o pedido deve ser de quinze (15) dias úteis a contar do dia seguinte à data do recebimento. Quando não for possível atender o pedido dentro desse prazo, o interessado será informado dos motivos da demora e da data em que o pedido será atendido, que em nenhum caso poderá exceder oito (8) dias úteis após o vencimento do primeiro termo. O pedido de exclusão da informação e a revogação da autorização não serão realizados quando o titular tiver um dever legal ou contratual com a empresa X, conforme termos acima.

## 7 ÁREAS DE PROTEÇÃO DE DADOS PESSOAIS

A empresa X tem uma unidade encarregada da recepção e atenção das petições, queixas e reclamações relacionadas aos Dados Pessoais: Serviço ao Cliente. Dentro desta unidade, o Serviço ao Cliente processará consultas e reivindicações relativas a Dados Pessoais de acordo com procedimentos internos e este conjunto de diretrizes.

## 8 VIGÊNCIAS

Este conjunto de diretrizes entrará em vigor a partir de janeiro de 2018. Os dados pessoais armazenados, utilizados ou transmitidos permanecerão nos bancos de dados da empresa X, com base no critério da temporalidade, desde que seja

necessário cumprir os propósitos mencionados neste documento, para os quais foram coletados. Assim, a validade dos bancos de dados da empresa X está intimamente relacionada aos propósitos para os quais os Dados Pessoais foram coletados.

## 9 OUTRAS DISPOSIÇÕES

A transferência de dados está coberta pelo contrato firmado da matriz com suas filiais em que os dados devem ser tratados e mantidos pela mesma, bem como na autorização do titular esse contrato é firmado também com o conhecimento do mesmo.

A empresa X não pretende coletar dados pessoais confidenciais de crianças ou menores.

Este documento pode ser modificado de tempos em tempos pela empresa X e deve fazer parte dos contratos celebrados pela mesma, quando aplicável. Qualquer modificação substancial deverá ser comunicada antecipadamente aos Titulares por meio de mecanismos eficientes, como o site e/ou e-mails. Modificação substancial significa, entre outras, as seguintes situações:

- Modificação na identificação da área, dependência ou pessoa encarregada de atender às consultas e reivindicações.
- Alteração clara dos propósitos que podem afetar a autorização concedida pelo titular.